RECEIVED CENTRAL FAX CENTER APR 1 1 2007

LISTING OF THE CLAIMS

- 1. (Currently Amended) A method for protecting data 1 generated by a keyboard, comprising the steps of: 2 reading data from a keypad of the keyboard; 3 reading an encryption seed from a device reader connected to the keyboard; 5 encrypting the read data using the encryption seed; 6 and 7 transmitting the encrypted data from the keyboard to a 8 computer. 2. (Original) The method of claim 1 further comprises the step's of receiving the transmitted encrypted data by the 2 computer; and 3 decrypting the received encrypted data by the computer. 5 3. (Original) The method of claim 1 wherein the step of transmitting comprises the step of using a wireless link over 2 which the encrypted data is transmitted. 3 4. (Canceled)
 - 2 -

- 5. (Canceled)
- 6. (Canceled)
- 7. (Currently Amended) The method of claim [6] 1
- wherein the step of reading the encryption seed comprises the
- 3 step of enabling the device reader with a personal identification
- 4 number.

1

- 8. (Canceled)
- 9. (Currently Amended) The method of claim 8
- 2 wherein the step of receiving the start signal comprises the step
- 3 of A method for protecting data generated by a keyboard,
- 4 comprising the steps of:
- 5 generating the a start signal by at least one of a
- 6 special key on keyboard [,] or multi-actuation of a number of
- 7 keys on the keypad, the computer, or a server
- 8 reading data from a keypad of the keyboard;
- encrypting the read data in response to the start
- 10 signal; and
- transmitting the encrypted data from the keyboard to a
- 12 computer.
- 1 10. (Currently Amended) The method of claim 1
- 2 wherein the step of encrypting comprises the step of

3	A method for protecting data generated by a
4	keyboard, comprising the steps of:
5	reading data from a keypad of the keyboard;
6	encrypting the read data in response to the start
7	signal; and
8	transmitting the encrypted data from the keyboard to a
9	computer
0	receiving a stop signal;
1	stopping the encryption of the read data and
2	transmission of the encrypted data from the keyboard to the
3	computer that stops the encryption.
1	11. (Currently Amended) The method of claim 10
2	wherein the step of receiving the stop signal comprises the step
3	of generating the stop signal by at least one of a special key on
4	keyboard [,] or multi-actuation of a number of keys on the
5	keypad, the computer, or a server.
1	12. (Canceled)
1	13. (Currently Amended) A method for protecting by
2	a computer data generated by a keyboard where the keyboard
3	is directly connected to the computer, comprising the steps of:
4	receiving encrypted data from the keyboard by the
5	computer; and
6	decrypting the encrypted data by the computer.

2

- 14. (Original) The method of claim 13 wherein the 1 step of decrypting comprises the step of performing operations
- of decryption by at least one of a keyboard driver executing on
- the computer or an application executing on the computer.
- 15. (Original) The method of claim 13 wherein the 1
- step of decrypting comprises the step of using a seed. 2
- 16. (Original) The method of claim 15 wherein the 1
- step of using comprises the step of reading the encryption seed
- from a device reader connected to the computer.
- 17. (Original) The method of claim 16 wherein the 1
- step of reading the encryption seed comprises the step of 2
- enabling the device reader with a personal identification
- number.
- 18. (Original) The method of claim 13 further
- comprises the step of generating a start signal to cause the 2
- keyboard to start encrypting data. 3
- 19. (Original) The method of claim 13 further
- comprises the step of generating a stop signal to cause the
- keyboard to stop encrypting data.

- 20. (Original) The method of claim 13 further comprises the step of transmitting program information to the keyboard to define encryption operations.
- 1 21. (Canceled)
- 1 22. (Canceled)
- 1 23. (Canceled)
- 1 24. (Canceled)
- 1 25. (Canceled)
- 26. (Currently Amended) A keyboard for encrypting data before transmission to a computer <u>directly</u> connected to the keyboard via a link, comprising:
- an interface connected to the link;
- s a memory;
- a keypad for generating the data;
- a device reader for reading a directly connected
- 8 device to obtain a seed for an encryption routine;
- a processor for encrypting <u>using the seed</u> the
- generated data by execution of [an] the encryption routine
- stored in the memory; and

3039209113

- transmitting the encrypted data to the computer via the interface and link.
- 1 27. (Original) The keyboard of claim 26 wherein the
- 2 link is a wireless link.
- 1 28. (Canceled)
- 29. (Canceled)
- 1 30. (Original) The keyboard of claim 26 comprises a
- 2 special key which when actuated causes the processor to at
- 3 least start executing the encryption routine or stop executing
- 4 the encryption routine.
- 1 31. (Currently Amended) A processor-readable
- 2 medium for protecting data generated by a keyboard,
- 3 comprising processor-executable instructions configured for:
- reading data from a keypad of the keyboard;
- reading an encryption seed from a device reader
- 6 connected to the keyboard;
- 7 encrypting the read data <u>using the encryption seed;</u>
- 8 and
- transmitting the encrypted data from the keyboard to a
- 10 computer.

- 1 32. (Original) The processor-readable medium of
- 2 claim 31 wherein the transmitting comprises using a wireless
- 3 link over which the encrypted data is transmitted.
- 1 33. (Canceled)
- 1 34. (Canceled)
- 1 35. (Canceled)
- 36. (Currently Amended) The processor-readable
- 2 medium of claim 35 31 wherein the reading the encryption seed
- 3 comprises enabling the device reader with a personal
- 4 identification number.
- 37. (Canceled)
- 1 38. (Currently Amended) The processor-readable
- 2 medium of claim 37 wherein the start signal is generated A
- 3 processor-readable medium for protecting data generated by a
- 4 keyboard, comprising processor-executable instructions
- 5 configured for:
- 6 generating the <u>a</u> start signal by at least one of a
- 7 special key on keyboard [,] or multi-actuation of a number of
- 8 keys on the keypad, the computer, or a server
- 9 reading data from a keypad of the keyboard;

0	encrypting the read data in response to the start
1	signal; and
2	transmitting the encrypted data from the keyboard to a
3	computer.
1	39. (Currently Amended) The processor-readable
2	medium of claim 31 wherein the encrypting comprises A
3	processor-readable medium for protecting data generated by a
4	keyboard, comprising processor-executable instructions
5	configured for:
6	reading data from a keypad of the keyboard;
7	encrypting the read data in response to the start
8	signal; and
9	transmitting the encrypted data from the keyboard to a
0	computer
1	receiving a stop signal;
2	stopping the encryption of the read data and
3	transmission of the encrypted data from the keyboard to the
4	computer that stops the encryption.
1	40. (Currently Amended) The processor-readable
2	medium of claim 39 wherein the the stop signal generated by at
3	least one of a special key on keyboard [,] or multi-actuation of a
4	number of keys on the keypad, the computer, or a server.
1	41. (Canceled)

- 1 42. (Original) An apparatus for executing the steps of
- claim 1.
- 1 43. (Original) An apparatus for executing the steps of
- 2 claim 2.
- 1 44. (Currently Amended) An apparatus for executing
- 2 the steps of claim [4] 9.
- 1 45. (Currently Amended) An apparatus for executing
- 2 the steps of claim [5] <u>10</u>.
- 1 46. (Canceled)
- 1 47. (Canceled)
- 1 48. (Currently Amended) An apparatus for executing
- 2 the steps of claim [12] <u>11</u>.